CLAIMS:

What is claimed is:

1. A method for enabling privileges comprising:

establishing a session on behalf of a user;

receiving a request to enable database privileges for the user;

verifying trusted security logic has been executed prior to receiving the request to enable database privileges; and

enabling database privileges for the user if the trusted security logic has been executed prior to receiving the request to enable the database privileges.

2. The method of claim 1, further comprising:

storing call information in one or more frames of a call stack; and wherein

the act of verifying comprises determining whether the one or more frames of the call stack corresponds to the trusted security logic.

3. The method of claim 1, wherein the act of verifying the trusted security logic comprises verifying an application name.

4. The method of claim 3, wherein the act of verifying the trusted security logic further includes verifying a security function name.

5. The method of claim 1, wherein the act of verifying trusted security logic comprises verifying a module name.

6. The method of claim 1, further comprising:

collecting one or more session parameters;

comparing the one or more session parameters against a set of trusted security parameters defined in a security function; and

returning a result indicating whether the one or more session parameters matches the set of trusted security parameters.

7. The method of claim 1, wherein the act of verifying the trusted security logic comprises verifying a proxy user.

8. The method of claim 1, further comprising:

receiving information identifying the user;

prompting the user for a password;

authenticating the user based on information stored in an application program; and

associating the user with a role.

9. A client-server computer system comprising:

a computer including:

a processor,

a main memory communicatively coupled to the processor; and

a disk storage communicatively coupled to the processor;

a database running on the computer from the main memory, the database further comprising:

one or more data structures stored in the disk storage, and

a call stack stored in the main memory;

an application program coupled to the database and configured to support a user; and

a metadata repository embodied in the one or more data structures stored in the disk storage, the metadata repository comprising trusted security logic; wherein

the application program is configured to initiate a call to enable database privileges, the call causing call information to be stored in one or more frames of the call stack and one or more security functions to be executed; and wherein

the database is configured to:

verify the call stack comprises one or more frames corresponding to the trusted security logic; and

enable database privileges for the user if the trusted security logic is contained in the one or more frames.

10. The client-server computer system of claim 9, wherein the application program resides with the database in the computer.

11. The client-server computer system of claim 9, wherein the application program resides on a separate computer communicatively coupled to the database.

12. The client-server computer system of claim 9, wherein the trusted security logic includes a schema name and a security package name.

13. The client-server computer system of claim 9, wherein verifying further includes testing a proxy user.

14. A computer-readable medium have stored therein one or more sequences of instructions for enabling privileges, the one or more sequences of instructions causing one or more processors to perform a number of acts, said acts comprising:

establishing a session on behalf of a user;

receiving a request to enable database privileges for the user;

verifying trusted security logic has been executed prior to receiving the request to enable database privileges; and

enabling database privileges for the user if the trusted security logic has been executed prior to receiving the request to enable the database privileges.

15. The computer-readable medium of claim 14, further comprising:

storing call information in one or more frames of a call stack; and wherein

the act of verifying comprises determining whether the one or more frames of the call stack corresponds to the trusted security logic.

16. The computer-readable medium of claim 14, wherein the act of verifying the trusted security logic comprises verifying an application name.

17. The computer-readable medium of claim 16, wherein the act of verifying the trusted security logic further includes verifying a security function name.

18. The computer-readable medium of claim 14, wherein the act of verifying trusted security logic comprises verifying a security function name.

19. The computer-readable medium of claim 14, further comprising:

collecting one or more session parameters;

comparing the one or more session parameters against a set of trusted security parameters defined in a security function; and

returning a result indicating whether the one or more session parameters matches the set of trusted security parameters.

20. The computer-readable medium of claim 14, wherein the act of verifying the trusted security logic comprises verifying a proxy user.

21. The computer-readable medium of claim 14, further comprising:

receiving information identifying the user;

prompting the user for a password;

authenticating the user based on information stored in an application program; and

associating the user with a role.

22. A method for enabling privileges comprising:

receiving a request to enable a role;

generating a list of security policies associated with the role, the list of security policies selected from a metadata repository;

executing each security policy identified in the list;

returning a value indicating a successful or unsuccessful execution of each security policy; and

enabling database privileges associated with the role if the value returned by all the executed security policies indicates each was successful.

23. The method of claim 22, wherein said act of executing each security policy comprises:

collecting one or more session parameters; and

comparing said one or more session parameters to authorized session parameters specified in the security policy.

24. The method of claim 22, wherein said act of executing each security policy comprises verifying one or more frames in a call stack corresponds to trusted security logic stored in the metadata repository.

25. The method of claim 22, wherein said act of executing each security policy comprises verifying a proxy user.